UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/589,552	08/16/2006	Giovanni Ghigo	09952.0069	8465

22852 7590 09/04/2008

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER	
WRIGHT, BRYAN F	

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
09/04/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/589,552	GHIGO ET AL.	
	Examiner	Art Unit	
	BRYAN WRIGHT	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 August 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *19-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *19-36* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 August 2006* is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *8/16/2006*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to application file on August 16, 2006. Claims (19-36) are pending.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 19-36 are rejected under 35 U.S.C. 102(b) as being anticipated by Chiu et al. (US Patent No. 4,667,301 and Chiu hereinafter).

3. As to claim 19, Chiu teaches a **random number generator, comprising:**

a true random number generator (i.e., ...teaches provides for a random number generator (col. 1, lines 55-60);

a pseudo-random number generator arranged to generate a pseudo-random sequence by using the true random numbers produced by said true random number generator as random seed (i.e., ... further teaches a array of multiplication complexes produces the next k consecutive pseudo-random numbers in the sequence and back into the array of k registers simultaneously [col. 7, lines 35-40] ...teaches a generation process is initiated with a starting number Z.sub.o, also known as a seed [col. 2, lines 45-50]);

and a mixing logic connected between said true random number generator and said pseudo-random number generator and arranged to alter the behavior of said pseudo-random number generator by using the random seed (i.e., ...teaches a main control 412 for controlling the flow of random numbers [col. 8, lines 35-45] ... further teaches a generation process is initiated with a starting number Z.sub.o, also known as a seed [col. 2, lines 45-50]), **said true random generator being arranged to generate a random sequence of bits having variable rate** (i.e., ...teaches The number of bits of the intermediate product is then reduced to that specified for each PRN through an inverse transform network, thereby forming a new PRN [abstract]), **and said mixing logic comprising a generator of an alteration signal intended to change the behavior of said pseudo-random number generator at multiple random instants in the interval between two subsequent seeds** (i.e., a pulse generator or clock signal from main control 412 for sequencing all events in order [col. 7, lines 35-45]), **thereby obtaining in said interval multiple pseudo-random sequences of random lengths shorter than the random length determined by the arrival of two subsequent seeds** (i.e., ...teaches the closer s' is to s the better, preferably s'=s+1 [col. 5, lines 60-65]), **said generator of the alteration signal being connected so as to receive said seed and generate said alteration signal by processing said seed by means of the sequence generated by said pseudo-random number generator** [fig. 5].

4. As to claim 20, Chiu teaches a **random number generator as claimed in claim 19, wherein said generator of the alteration signal comprises:**

a first down counter arranged to count down from a first random number represented by a first group of bits which are part of a randomly rotated version of a seed received by said alteration signal generator (i.e., ... teaches number control consists of a counter 422 and a decoder 424 which produces a count indicative of the number of particular fleet random numbers generated in register [col. 9, lines 1-11]), **said first counter loading said first random number and starting its countdown whenever a seed is available and** (i.e., ... teaches a number counter to produce an output count as each new random number is formed [claim 1]), **between the occurrence of two subsequent seeds, whenever it generates a terminal count signal, said terminal count signal being fed to said pseudo-random number generator as alteration signal** (i.e., ...teaches a main control 412 for controlling the flow of random numbers [col. 8, lines 35-45] ... further teaches a generation process is initiated with a starting number Z.sub.o, also known as a seed [col. 2, lines 45-50]) ;

a second down counter which is arranged to count down from a second random number represented by a group of bits of the sequence generated by said pseudo-random number generator and is arranged to load a new value of said second random number and to start again its countdown whenever said first down counter generates its terminal count signal (i.e., ... teaches a systolic control consists of a counter and a decoder, which counts the number of iterations performed by multiplication slice and creates a new output bit from decoder to be

coupled to the multiplexer at the same time the multiplication slice produces a new output bit [col. 8, lines 55-67]);

and a recirculating shift register which receives the seeds and feeds said first down counter with said first random number, and which is arranged to generate said randomly rotated version of the seed in the intervals between the arrivals of two subsequent seeds by rotating the bits of the seed by an amount determined by the value of said second random number (i.e., ... teaches the input operand bits of a are fed only initially into the registers 36-58 thru lines 12-34. ... teaches will then proceed just as described above and yield a bit of product in that machine cycle. ... teaches in the second cycle, the lines 12-34 are disabled and the content of registers 36-58 is cyclically shifted leftward thru lines 512, 514, . . . 534 and the signals proceed in the above mentioned manner to generate a second bit of product [col. 5, lines 30-40] [fig. 2]).

5. As to claim 21, Chiu teaches a **random number generator where said pseudo-random generator is a linear feedback shift register and said alteration signal generator supplies said alteration signal to the feedback logic of said linear feedback shift register** [col. 5, lines 30-40].

6. As to claim 22, Chiu teaches a **random number generator where said mixing logic further comprises an input circuitry arranged to receive the random sequence of bits generated by said true random generator to build said seed by**

parallelising the bits of said random sequence and to generate a signal indicating the availability of a seed (i.e., ... teaches to generate pseudo-random numbers, at high speed using parallelism [col. 2, lines 1-5])

7. As to claim 23, Chiu teaches a **random number generator where said recirculating shift register is arranged to load a seed directly whenever it receives said signal indicating the availability of the seed** (i.e., ... teaches a feedback configuration of the shift register is determined by M and a shift toward the high order bit position is mathematically a multiplication, by x, of the polynomial originally in the feedback shift register [col. 6, lines 15-30]), **and said pseudo-random generator is arranged to load a new seed upon command of said first counter whenever the latter receives said signal indicating the availability of the seed** (i.e., ... teaches recognizing the recursiveness inherent in the pseudo-random number sequence [col. 5, lines 50-65]).

8. As to claim 24, Chiu teaches a **random number generator where said input circuitry comprises a clock signal generator for generating, starting from a first clock signal timing the operations of said input circuitry, and a second clock signal for timing said pseudo-random generator and said alteration signal generator whereby the output bit rate of the random number generator is independent of the rate of the random sequence of bits supplied by the true**

random generator (i.e., ... teaches a pulse generator or clock signal from main control for sequencing all events in order [col. 8, lines 35-45])

9. As to claim 25, Chiu teaches a **random number generator further comprising an output logic for parallelising the altered pseudo-random sequence and building words of a given length** (i.e., ...teaches the parallel generation of multiple pseudo-random numbers per machine cycle [fig. 3]) ... further teaches a pseudo-random numbers vector can be generated truly in parallel with a segment of k elements simultaneously at one time [col. 7, lines 50-60]), **said output logic comprising a scrambler for scrambling the bits in each word in random manner** [col. 4, lines 35-45].

10. As to claim 26, Chiu teaches a **random number generator where said scrambler is controlled by a random selection signal provided by said generator of the alteration signal** [fig. 3].

11. As to claim 27, Chiu teaches a **random number generator where a random selection signal is supplied by said recirculating shift register** (i.e., ... teaches main control controls the beginning and ending of the random number generation process, as the result of control signals from a central processor unit. ... teaches a main control is connected to a systolic control, which controls the register control for the

generation of particular random numbers generated by multiplication slice [col. 8, lines 50-60]).

12. As to claim 28, Chiu teaches a **random number generator as claimed in claim 25, wherein said scrambler circuit comprises a switching matrix comprised of an n-level binary tree of switches, each controlled by a respective bit of said random selection signal so as to scramble or to let through unchanged its input bits** [fig. 4].

13. As to claim 29, Chiu teaches a **random number generator implemented as an integrated circuit** [fig. 2c].

14. As to claim 30, Chiu teaches a **method of generation of random numbers, in which said random numbers are generated by altering a pseudo-random sequence by means of true random numbers forming random seeds for the generation of said pseudo-random sequence** [col. 2, lines 45-50]**, the method comprising the steps of:**

obtaining the random seeds from a random sequence of bits having variable rate (i.e., ...teaches The number of bits of the intermediate product is then reduced to that specified for each PRN through an inverse transform network, thereby forming a new PRN [abstract]); processing a random seed to generate an alteration signal exploiting the random arrival time of the bits of said sequence of bits;

and changing the pseudo-random sequence by said alteration signal at random instants between the arrival of two subsequent seeds [fig. 3], **thereby obtaining in said interval multiple pseudo-random sequences of random lengths shorter than the lengths determined by the arrival of two subsequent seeds** [fig. 4], **said alteration signal being generated under the control of the pseudo-random sequence** [fig. 2b].

15. As to claim 31, Chiu teaches a **method where said alteration signal is generated at the end of a first countdown starting from a first random number represented by a randomly variable group of bits that are part of a rotated version of a received seed obtained by rotating the seed by an amount indicated by a second random number represented by a group of bits of the pseudo-random sequence, the first countdown starting whenever a seed is generated and restarting, between the arrival of two subsequent bits, whenever the countdown itself ends** [col. 4, lines 60-67; col. 5, lines 1-30];

and where said second random number is the starting value of a second countdown starting whenever the first down counting ends, the end of said second countdown stopping said seed rotation [fig. 3].

16. As to claim 32, Chiu teaches a **method where said pseudo-random sequence is generated by a linear feedback shift register and said alteration signal is fed to the feedback logic of said linear feedback shift register** (i.e., ... teaches a small

number of shifts, like 5, to shift however, a combined feedback network can be realized in a single operation within one machine cycle [col. 6, lines 39-48]).

17. As to claim 33, Chiu teaches a **method where the altered pseudo-random sequence is parallelised to create words of a desired length and further comprising a random scrambling of said words** [col. 4, lines 35-45].

18. As to claim 34, Chiu teaches a **method where said scrambling is controlled by a random selection signal obtained from the bits used to form said first random number** [col. 4, lines 30-45].

19. As to claim 35, Chiu teaches a **method further comprising the step of generating, starting from a first clock signal timing the seed generation and a second clock signal for timing the generation of said pseudo-random sequence and of said alteration signal, the parallelisation of the output words and the scrambling, whereby an output bit rate independent from the rate of the random sequence of bits is obtained** (i.e., ... teaches a pulse generator or clock signal from main control for sequencing all events in order [col. 8, lines 35-45]).

20. As to claim 36, Chiu teaches a **computer program product loadable in the memory of at least one computer and including software code portions capable of performing the method of claim 30** [col. 2, lines 1-5].

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRYAN WRIGHT whose telephone number is (571)270-3826. The examiner can normally be reached on 8:30 am - 5:30 pm Monday -Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, AYAZ Sheikh can be reached on (571)272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BRYAN WRIGHT/
Examiner, Art Unit 2131

/Ayaz R. Sheikh/
Supervisory Patent Examiner, Art Unit 2131